REMARKS

This Amendment is fully responsive to the non-final Office Action dated December 5, 2008, issued in connection with the above-identified application. Upon entry of this Amendment, claims 16, 17, 22 and 23 have been canceled without prejudice or disclaimer to the subject matter therein; claims 1, 2, 5, 9-11, 14, 18, 20 and 21 have been amended, and claim 24 has been added. Claims 1-15, 18-21, and 24 are now currently pending in the present application. The claim amendments presented herein merely clarify the subject matter recited in the rejected claims, and are not meant to narrow the scope of the present invention. No new matter has been introduced by the amendments made to the claims or by the new claim added. Favorable reconsideration and further examination are respectfully requested.

I. Claim Objections

In the Office Action, claims 1-2, 5, 10, 14, 18 and 20-21 are objected to because of minor informalities. In particular, the Examiner alleges that the limitation "a random information generation unit operable to read the management information from the management information storage unit, and generate random information R based on the read management information" should read "a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information."

The Applicants have amended claims 1-2, 5, 10, 14, 18 and 20-21 to recite therein "a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information," as suggested by the Examiner. Thus, withdrawal of the objection to claims 1-2, 5, 10, 14, 18 and 20-21 is respectfully requested.

In the Office Action, claim 10 has been objected to for being dependent on a rejected based claim, but would be allowable if rewritten in independent form to include all the features of the base claim and any intervening claims. The Applicants have amended claim 10, as suggested by the Examiner. Accordingly, withdrawal of the objection to claim 10 is respectfully requested.

II. Claim Rejections under 35 U.S.C. 101

Claim 20-21 and 23 are rejected under U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The Examiner alleged that claim 20 lacks a useful result in order to accomplish a practical application. The Applicants have amended claim 20 to include a useful result of the prime calculation method therein. Thus, the Applicants respectfully request that the rejection to claim 20 under 35 U.S.C. 101 be withdrawn.

With regard to claims 21 and 22, the Examiner alleged that the claim 21 lacks the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 U.S.C. 101. The Applicants have amended claim 21 to clarify that the program is stored on "a computer-readable medium," and have canceled claim 22. Thus, the Applicants respectfully request that the rejection to claims 20 and 21 under 35 U.S.C. 101 be withdrawn.

With regard to claim 23, the Examiner alleges that claim 23 could include a carrier wave, and a carrier wave does not have any physical structure and thus does not fit within the definition of a machine or an article of manufacture. By the present amendments, the Applicants have canceled claim 23. Thus, the Applicants respectfully request that the rejection to claim 23 under 35 U.S.C. 101 be withdrawn.

III. Double Patenting

In the Office Action, claims 1-15 and 18-23 are provisionally rejected on the grounds of non-statutory obviousness-type double patenting as being un-patentable over claims 1-36 of co-pending Application No. 10/582,999.

The Applicants have filed herewith a terminal disclaimer in compliance with 37 C.F.R. 1.321(c) to obviate the judicially created double patenting rejection. The terminal disclaimer includes a provision that any patent granted on the present application shall be enforceable only for and during such period that said patent is commonly owned with the application or patent which formed the basis for the rejection. Thus, the Applicants respectfully request that the rejection to claims 1-15 and 18-23 based on the grounds of non-statutory obviousness-type double patenting be withdrawn.

IV. Claim Rejections under 35 U.S.C.§ 103

In the Office Action, claims 1-9, 11-15, 18, and 20-23 have been rejected under 35 U.S.C. 103(a) as being unpatentable over the Applicant Admitted Prior Art (hereafter "the AAPA") in view of Peyravian et al. ("Generation of RSA keys That Are Guaranteed to be Unique for Each User, " hereafter "Peyravian"). The Applicants respectfully traverse the above rejection for at least the reasons noted below. Specifically, the Applicants have canceled claims 22 and 23 thereby rending the above rejection to those claims moot. Additionally, the Applicants maintain that the cited prior art fails to disclose or suggest at least all the features of independent claims 1, 18, 20 and 21.

For example, independent claim 1 recites a prime calculating apparatus for calculating a prime candidate N larger than a known prime q and testing primality of the calculated prime candidate N, comprising: a prime storage unit storing the known prime q; a management information storage unit storing unique management information; a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information; a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N using the read prime q and the generated random information R, according to N=2 x random information R x prime q + 1; a primality testing unit operable to test primality of the calculated prime candidate N; and an output unit operable to output the calculated prime candidate N as a prime N when the primality of the calculated prime candidate N is determined.

The above features of independent claim 1 are similarly recited in independent claims 18, 20 and 21. Additionally, the features noted above are fully supported by the Applicants' disclosure.

In the Office Action, the Examiner relies on the AAPA in view of Peyravian for disclosing or suggesting all the features recited in independent claims 1, 18, 20 and 21. However, the Applicants respectfully asset that the applied prior art references do not teach or suggest the above-noted combination of features recited in independent claims 1, 18, 20 and 21.

Regarding the AAPA, the Examiner admits (i.e., in Official Action dated on December 5, 2008) that the AAPA fails to disclose at least a management information storage unit storing unique management information, and a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information. For these dependencies, the Applicants submit that the AAPA also fails to disclose a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N using the read prime q and the generated random information R, according to N=2 x random information R x prime q + 1.

Thus, independent claims 1, 18, 20 and 21 are clearly distinguished over the AAPA.

However, in setting forth the rejection, the Examiner relies on Peyravian regarding that which the Examiner admits is lacking in the AAPA.

However, Peyravian fails to disclose at least: a random information generation unit operable to read the unique management information from the management information storage unit, and generate random information R based on the read unique management information; and a candidate calculation unit operable to read the prime q from the prime storage unit, and calculate the prime candidate N using the read prime q and the generated random information R, according to N=2 x random information R prime q + 1.

Rather, Peyravian merely teaches that a prime pair (p, q) is generated, using user-specific data (unique management information) B, within an interval of $2^{n-1}(1+B/2^b)$ and $2^{n-1}(1+(B+1)/2^b)$ (see page 285, lines 26-41), and primes p and q are selected from the above interval (see page 285, lines 43-44).

In other words, Peyravian does not contain any disclosures regarding a random information generation unit that generates random information R based on the read unique management information. Instead, Peyravian merely teaches that the interval of $2^{n-1}(1+B/2^b)$ and $2^{n-1}(1+(B+1)/2^b)$ is created using the user-specific data (unique management information) B (see page 285, lines 26-41). Peyravian also does not contain any disclosure regarding a candidate calculation unit that is operable to read the prime q from the prime storage unit, and to calculate the prime candidate N using the read prime q and the generated random information R,

according to N=2 x random information R x prime q + 1. Instead, Peyravian merely teaches that primes p and q are selected from the above interval (see page 285, lines 43-44).

Thus, Peyravian does not contain any disclosures regarding the combinations of the above features recited in independent claims 1, 18, 20 and 21. Therefore, the Applicants submit that even if one of ordinary skill in the art were to combine the teaching of the AAPA with Peyravian, the combination still fails to arrive at the present invention. As such, the combination of the AAPA and Peyravian would lack, at least, the above combinations of the features of the present invention (recited in independent claims 1, 18, 20 and 21.

Based on the above discussion of the cited prior art, no combination of the AAPA and Peyravian would result in, or otherwise render obvious, independent claims 1, 18, 20 and 21. Likewise, no combination of the AAPA and Peyravian would result in, or otherwise render obvious, claims 2-9 and 24 at least by virtue of their dependencies from independent claim 1. With regard to claims 11-15, the claims have been amended to depend from claim 10, which has been rewritten in independent form. As rewritten, claim 10 is now believed to be in condition for allowance. Accordingly, claims 11-15 should also be in condition for allowance at least by virtue of their dependencies from claim 10.

In the Office Action, claim 19 has been rejected under 35 U.S.C. 103(a) as being unpatentable over the AAPA in view of Peyravian, and further in view of Oka et al. (U.S. Publication No. 2002/0108042, hereafter "Oka").

Claim 19 depends from independent claim 18. As noted above, the AAPA in view of Peyravian fails to disclose or suggest all the features of independent claim 18. Additionally, Oka fails to overcome the deficiencies noted above in the AAPA in view of Peyravian. Accordingly, no combination of the AAPA, Peyravian and Oka would result in, or otherwise render obvious, claim 19 at least by virtue of its dependency from independent claim 18.

V. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Yuichi FUTA et al.

/Mark D. Pratt/
2009.03.05 16:15:41 -05'00'

By: _____
Mark D. Pratt
Registration No. 45794
Attorney for Applicants

MDP/ats
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
March 5, 2009